2. Indien derden werkzaamheden verrichten, b.v. i.h.k.v. onderhoud, wordt contractueel geregeld dat leveranciers geen gegevensdragers met data buiten het Belastingdienstdomein brengen.

Norm

DM N-1-4 B/CICT	De relatie tussen de leverancier en B/CICT is uitsluitend van zakelijke aard en mag niet beïnvloed worden door gunsten van welke aard ook.

Maatregelen

1. Indien leveranciers aan werknemers van B/CICT geschenken en/of gunsten aanbieden, en/of uitnodigingen via derden om een bijeenkomst (waaronder niet begrepen educatieve bijeenkomsten) bij te wonen, en/of op andere wijze voorrechten verlenenwordt de leverancier hierop aangesproken. In de leveranciers performance rapportage zal hiervan melding worden gemaakt.
2. Indien de leverancier volhardt in haar gedrag, zal de relatie met deze leverancier worden beëindigd.

2.2.6 Exploitatie

Richtlijn

EP R-1 B/CICT	*De ICT – services in productie dienen beschermd te worden tegen informatiebeveiligingsinbreuken.*

Risicoafweging

Bij het exploiteren van (ICT-)services bestaat het risico dat de informatiebeveiliging van (*ICT-) Services* bewust of onbewust voor korte of langere termijn negatief wordt beïnvloed en zo de *informatiebeveiliging* van de Belastingdienst in gevaar brengt.

Norm

EP N-1-1 B/CICT	In de *productie- en acceptatietestomgeving* zijn geen andere specifieke middelen aanwezig dan die door het proces O&B zijn opgeleverd

Maatregelen

1. Periodiek vindt er een software-inventarisatie plaats op basis van bestandscatalogi uit de systemen, waarbij vastgesteld wordt dat alleen die middelen aanwezig dan die door het proces O&B zijn opgeleverd.
2. Speciale maatregelen die zijn gevraagd vanuit O&B in verband met risico's die kunnen worden veroorzaakt door applicaties die door hun aard de *integriteit* of vertrouwelijkheid van de TIS en/of data kunnen beïnvloeden, worden opgevolgd. Hierbij kan gedacht worden aan applicaties die ingezet kunnen worden voor andere doeleinden dan waar ze oorspronkelijk voor zijn bedoeld (bv. Sniffers, querytools, BI-tooling etc.).

Norm

EP N-1-2 B/CICT	De middelen voor het opslaan van data en het verwerken daarvan zijn altijd zo uitgevoerd dat in het geval van een *calamiteit* het opslaan en verwerken ongestoord doorgang kan vinden.

Maatregelen

1. Voor data- en programmatuur bestanden functioneren automatisch werkende dupliceermechanismen die op een van de productie gescheiden locatie(s) geplaatst zijn. Dit geldt inclusief de (elektronische) systeemdocumentatie. De gescheiden locatie(s) voldoen aan dezelfde eisen als van de productielocatie.
2. Er worden op de gedupliceerde data geen andere toegangsrechten toegekend dan nodig is om in geval van *calamiteiten* de benodigde activiteiten te kunnen uitvoeren.

Norm

EP N-1-3 B/CICT	Uitwijktesten mogen geen afbreuk doen aan de *integriteit* en vertrouwelijkheid van de *productiegegevens*.

Maatregelen

1. Bij uitwijktesten wordt voor het testen van mutatiefuncties altijd uitgegaan van kopieën van productiedata.
2. Door een onafhankelijke informatiebeveiligingsfunctionaris wordt vooraf getoetst of het ontwerp van de uitwijktest borgt dat er geen oneigenlijke mutaties in productiegegevens aangebracht kunnen worden.

300939 0085

3. Door een onafhankelijke informatiebeveiligingsfunctionaris wordt getoetst of het uitvoeren van uitwijktesten mogelijk afbreuk kan doen aan het handhaven van het Basis Beveiligings Niveau.
4. Na afloop van de test wordt een print-out van de bestandscatalogus aan het uitwijktestdossier toegevoegd, waaruit blijkt dat er op de gebruikte computersystemen – na dato van de test – geen data meer zijn achtergebleven.

Norm

EP N-1-4 B/CICT	Beveiligingsrisico' s worden vastgelegd, tijdig geanalyseerd en afgehandeld.

Maatregelen

1. De Beveiligingsrisico's worden vastgelegd, tijdig geanalyseerd en afgehandeld door de *Medewerker monitoring beveiliging* , onafhankelijk van de functie die verantwoordelijk is voor het *operationeel beheer*.
2. Door de *Security Specialist* wordt er achteraf op toegezien dat de afhandeling van de gesignaleerde afwijkingen juist en tijdig plaatsvindt.
3. Beveiligingsrisico's die niet binnen de daarvoor opgestelde termijn zijn opgelost worden geëscaleerd naar de *beveiligingscoördinator* van B/CICT.

Norm

EP N-1-5 B/CICT	Beveiligingsinstellingen van *(ICT-)services* worden regelmatig op juistheid getoetst.

Maatregelen

1. De beveiligingsinstellingen van de in het proces Architectuur aangewezen en in het proces O&B uitgewerkte *TIS-componenten* worden getoetst volgens de bij het ontwerp behorende technische documentatie, onafhankelijk van de functie die verantwoordelijk is voor het operationeel en logisch beheer.
2. Ingeval er automatische controles kunnen plaatsvinden, is er functiescheiding tussen degenen die de beveiligingsinstellingen van het normbestand kunnen muteren en degenen die de gesignaleerde afwijkingen afhandelen.
3. De activiteiten van medewerkers met hoge systeemrechten worden vastgelegd en periodiek geanalyseerd.
4. Door de *Security Officer* wordt er op toegezien dat de afhandeling van de gesignaleerde afwijkingen juist en tijdig plaatsvindt.
5. De mate waarin risicos worden gelopen, is bepalend voor de frequentie van de controle op beveiligingsinstellingen van de *(ICT-)services.*

Richtlijn

EP R-2 B/CICT	*De kritische ruimten , die onder beheer vallen van Exploitatie dienen beschermd te worden tegen informatiebeveiligingsinbreuken*

Risicoafweging

Het risico bestaat dat de informatiebeveiliging van *ICT-Service*s en gegevens bewust of onbewust voor korte of langere termijn negatief wordt beïnvloed en zo de *informatiebeveiliging* van de Belastingdienst in gevaar brengt.

300939 0085

Norm

EP N-2-1 B/CICT	*Kritische ruimten* worden zodanig beheerd, dat inbreuken op de vertrouwelijkheid, *integriteit* en beschikbaarheid worden voorkomen.

Maatregelen

1. Vanuit het exploitatieproces (proces operations) wordt gezorgd dat, óf in de SNO met B/CFD met betrekking tot kritische ruimtes wordt vastgelegd óf door medewerkers van exploitatie zelf wordt geregeld dat:
   1.1 De ruimte waarin de *ICT-componen*ten staan opgesteld voldoet aan voldoende eisen met betrekking tot toegangsbeveiliging, brandbeveiliging, beveiliging tegen blikseminslag en stroomstoringen zonder dat dit de ICT componenten in deze ruimten negatief beïnvloeden.
   1.2 Fotografische, video-, audio- of andere opnameapparatuur niet wordt toegestaan, tenzij hier goedkeuring voor is verleend door de beveiligingscoördinator.
   1.3 Het personeel alleen voor zover nodig is op de hoogte wordt gesteld van het bestaan van of de activiteiten binnen een kritische ruimte.
   1.4 Zonder toezicht werken in *kritische ruimten* wordt voorkomen, zowel om veiligheidsredenen als om de kans op kwaadwillige handelingen te voorkomen.
   1.5 Aan personeel van externe ondersteunende diensten alleen wanneer dit noodzakelijk is beperkte toegang wordt verleend tot *kritische ruimten* of voorzieningen waar gevoelige informatie wordt verwerkt.
   1.6 Standaardprocedures gelden voor de ontvangst en begeleiding van bezoekers waardoor de toegang tot en de daarin te verrichten menselijke activiteiten in deze ruimte tot een minimum wordt beperkt. Deze procedure wordt zonder uitzondering opgevolgd.
   1.7 Ongeautoriseerd gebruik van een toegangsmogelijkheid (bijvoorbeeld meelopen) wordt voorkomen.
   1.8 Alle toegang tot de kritische ruimtes wordt geregistreerd.
   1.9 Éénduidig is vastgelegd waar goederen, die in *kritische ruimten* worden gebruikt, worden ontvangen en uitgepakt.
   1.10 Binnenkomende materialen gecontroleerd worden op mogelijke gevaren voordat zij worden overgebracht van de voorraadruimte naar de kritische ruimte waar zij nodig zijn.
   1.11 Papierafval (zoals uitval en onjuiste uitvoer) regelmatig wordt afgevoerd naar een (brand)veilige plaats.
   1.12 Voor het afvoeren en vernietigen van papierafval geschikte bedrijven worden gekozen, die hier ervaring mee hebben en de nodige *informatiebeveiligingsmaatregelen* in acht nemen.
   1.13 Bij onderhoudswerkzaamheden, die aanwezigheid vereisen van medewerkers of derden die normaliter hun werkzaamheden niet in de *kritische ruimten* uitvoeren, de *informatiebeveiligingsmaatregelen* intact blijven. Als dit door omstandigheden niet mogelijk is, worden compenserende maatregelen getroffen om eventuele informatiebeveiligingsrisico's af te dekken.
   1.14 De werking van de fysieke *beveiligingsmaatregelen* (toegangsbeveiliging, brandbeveiliging, beveiliging tegen blikseminslag en stroomstoringen) regelmatig wordt getest. In de testplannen zijn speciale maatregelen genomen om ongeplande onbeschikbaarheid als gevolg van testwerkzaamheden te voorkomen.

300939 0085

Richtlijn

EP R-3 B/CICT	*Gegevens dienen beschermd te worden tegen inbreuken op vertrouwelijkheid en integriteit.*

Risicoafweging

Het risico bestaat dat ondanks algemene maatregelen van logische toegangsbeveiliging langs andere wegen de informatiebeveiliging van gegevens bewust of onbewust voor korte of langere termijn negatief wordt beïnvloed en zo de *informatiebeveiliging* van de Belastingdienst in gevaar wordt gebracht. Bovendien kan het bij het exploiteren van *ICT-Services* voorkomen dat daarbij klantgegevens mede geregistreerd worden. Voorbeelden daarvan zijn logginggegevens, autorisatiegegevens, incidentgegevens e.d. Deze gegevens kunnen soms misbruikt worden. Uit oogpunt van privacybescherming, beschreven in de wet bescherming persoonsgegevens (WBP), dienen hiervoor speciale informatiebeveiligingsmaatregelen te worden getroffen.

Norm

EP N-3-1 B/CICT	Het gebruik van algemene vraagtalen e.d. is zodanig aan voorwaarden gebonden dat deze nimmer inbreuk kunnen maken op de *integriteit* en vertrouwelijkheid van de *productiegegevens*.

Maatregelen

1. Eindgebruikers mogen de productiedata uitsluitend wijzigen met behulp van de daarvoor bedoelde programmatuur en niet met behulp van generieke hulpmiddelen zoals b.v. queryprogrammatuur.
2. Indien de ICT – service door technische redenen die door Architectuur zijn toegestaan wél vraagtalen bevat dienen in het proces Exploitatie de bij de ICT – service behorende maatregelen om risico's te beperken te worden gecontrolled.

Norm

EP N-3-2 B/CICT	De proceseigenaar Exploitatie wijst de medewerkers aan, die manipulaties op data uit mogen (laten) voeren volgens geautoriseerde schriftelijke opdracht van de eigenaar van de data.

Maatregelen

1. Alleen medewerkers die daarvoor door het bevoegde management zijn aangewezen, mogen datamanipulaties uitvoeren.
2. Voordat deze data (logging en events) ingezien mogen worden door andere medewerkers, moet vooraf schriftelijk toestemming worden verleend door het bevoegde management;
3. Het management houdt een registratie bij wie toegang heeft of heeft gehad tot deze data;
4. Het verwerken van opdrachten tot datamanipulaties wordt als apart werkproces gezien, waarover apart in de Service Niveau Rapportage wordt gerapporteerd.
5. Aan de eigenaar van de data wordt verzocht schriftelijk op te geven welke medewerkers bevoegd zijn om opdrachten tot *bestandsmanipulaties* in te dienen.
6. Jaarlijks wordt aan de eigenaar van de data een terugmelding gedaan van de bevoegde medewerkers met het verzoek schriftelijk te bevestigen dat de opgave juist is.
7. Bij het in behandeling nemen van opdrachten wegens *bestandsmanipulaties* wordt gecontroleerd of de aanvraag door de eigenaar van de data is geautoriseerd.

300939 0085

Norm

EP B/CICT N-3-3	Rechtstreekse ingrepen op de data door een medewerker moeten te allen tijde naar de oorsprong van de verandering zijn terug te voeren en inhoudelijk volledig aan de eigenaar van de data worden teruggemeld.

Maatregelen

1. Rechtstreekse ingrepen op de data door een medewerker kunnen alleen voorkomen na uitdrukkelijke toestemming van de eigenaar van de data. Tevens geeft de eigenaar van de data aan onder welke voorwaarden deze *bestandsmanipulaties* mogen geschieden.
2. De in de ICT – service voorziene programmatuur ter controle van de bestandsintegriteit levert rapportages op die aan de eigenaar van de data via de ICT – service beheerder ter beschikking wordt gesteld. Deze rapportages zijn op geen enkele manier door de uitvoerende exploitatiemedewerkers te beïnvloeden.
3. Van de ten onrechte aangebrachte wijzigingen worden al dan niet met behulp van geautomatiseerde hulpmiddelen verslagen met de gegevens voor en na deze wijzigingen in de data aan de eigenaar van de data ter beschikking gesteld.

Norm

EP B/CICT N-3-4	Het is niet toegestaan productiegegevens met *vertrouwelijke gegevens* voor welke doeleinden dan ook te gebruiken *buiten de door exploitatie beheerde omgevingen en zonder het treffen van extra informatiebeveiligingsmaatregelen*.

Maatregelen

1. Indien kopieën van productiegegevens voor testdoeleinden noodzakelijk zijn, wordt gecontroleerd dat de eigenaar van de data schriftelijke toestemming heeft gegeven.
2. Kopieën van productiedata worden uitsluitend in de *test- en acceptatieomgeving* ter beschikking gesteld.
3. Er gelden speciale gedragsregels over het omgaan met privacygevoelige gegevens, waarbij testmedewerkers erop worden gewezen dat testoutput niet de productieruimten mogen verlaten en deze output na gebruik wordt vernietigd.
4. De kopie productiedata worden na gebruik gewist.

Norm

EP B/CICT N-3-5	Voor het afgeven van data aan derden (incl. Belastingdienstmedewerkers) moet de eigenaar van de data toestemming verlenen.

Maatregelen

1. Bij het accepteren van werkopdrachten voor het afgeven van productiedata aan derden (incl. Belastingdienstmedewerkers) wordt gecontroleerd of de eigenaar van de data toestemming heeft verleend.
2. Bij het samenstellen van autorisatieprofielen wordt gewaarborgd dat er geen toegang tot eindgebruikerfuncties en productiegegevens van de primaire informatiesystemen van de Belastingdienst wordt verleend, tenzij de eigenaar van het desbetreffende *informatiesysteem* daarvoor schriftelijk goedkeuring heeft verleend.

300939 0085

3. Maatregelen die de eigenaar van de informatiesystemen neemt om gebruik van informatiesystemen door CICT te beperken of te controleren moeten door de klant opdrachtgever per geval aan CICT worden kenbaar gemaakt.
4. Onderzoek van data:
   4.1. Logging en events die privacy gevoelige data bevatten worden alleen ontsloten door medewerkers die daartoe door het management zijn aangewezen.
   4.2. Na vermoeden van plichtverzuim of strafbare feiten is er, op verzoek van de beveiligingscoördinator van B/CICT en na goedkeuring van het directoraat van de Belastingdienst (DGBel), onderzoek mogelijk naar personen (inclusief medewerkers van de Belastingdienst) in de bestanden van de Belastingdienst
   4.3. Deze onderzoeken worden uitgevoerd door of onder verantwoordelijkheid van de beveiligingscoördinator B/CICT door medewerkers die daartoe door het management zijn aangewezen.

Norm

EP B/CICT N-3-6	Indien ICT-apparatuur buiten werking wordt gesteld, wordt gecontroleeerd of de opgeslagen *productiegegevens* gewist zijn.

Maatregelen

1. Indien ICT-apparatuur tijdelijk buiten gebruik wordt gesteld, worden productiegegevens onherstelbaar gewist.
2. Voor het onherstelbaar wissen van gegevens wordt speciale software dan wel démagnetiseringsapparatuur gebruikt.
3. Bij het buiten gebruik stellen van ICT-apparatuur, wordt via het proces Inkoopmanagement en logistiek het onherstelbaar wissen van vaste schijven conform de regeling materieel beheer Rijksoverheid 2006, uitgevoerd.
4. Indien derden werkzaamheden verrichten, b.v. i.h.k.v. onderhoud, wordt gecontroleerd dat leveranciers geen gegevensdragers met data buiten het Belastingdienstdomein brengen.
5. Bij onderhoudswerkzaamheden waarbij gegevensdragers worden verwisseld, wordt de informatie op de oorspronkelijke gevensdrager verwijderd.

Norm

EP B/CICT N-3-7	Voor exploitatiedoeleinden verzamelde gegevens van klanten worden niet voor andere dan bedoelde doeleinden beschikbaar gesteld

Maatregelen

1. Aanvragen voor het ontsluiten en bewerken van voor exploitatiedoeleinden verzamelde gegevens van klanten worden goedgekeurd door de Voorzitter van het managementteam van B/CICT, nadat hij heeft vastgesteld dat daarvoor opdracht wordt gegeven door het bevoegd gezag.
2. De afhandeling van dergelijke opdrachten worden uitgevoerd onder direct toezicht van de beveiligingscoördinator van B/CICT.

300939 0085

Richtlijn

EP B/CICT R-4	*Bij de uitvoering van identificatie-, authenticatie- en autorisatiebeheer werkzaamheden dienen informatiebeveiligingsregels in acht te worden genomen.*

Risicoafweging

Het risico bestaat dat werkzaamheden in het kader van logische toegangsbeveiliging de informatiebeveiliging van (*ICT-)service*s en gegevens bewust of onbewust voor korte of langere termijn negatief beïnvloeden en zo de *informatiebeveiliging* van de Belastingdienst in gevaar brengt.

Norm

EP B/CICT N-4-1	Toegangsrechten worden alleen verleend, indien deze worden aangevraagd door de eigenaar van het autorisatieproces binnen de belastingdienst.

Maatregelen

1. Het aanbrengen van autorisaties voor alle medewerkers van de Belastingdienst behalve de beheerders van B/CICT gebeurt uitsluitend door B/CA.
2. Bij het opvoeren van autorisaties wordt ervoor zorggedragen dat er overeenstemming blijft bestaan met de autorisatieprofielen die door B/CA zijn vastgesteld, o.a. door een periodieke Soll-Ist vergelijking.
3. Indien wijzigingen in groepsautorisaties niet binnen het ontwerp van de groepsstructuur kunnen plaatsvinden, wordt dit tijdig gerapporteerd aan de *functioneel beheerder* van de desbetreffende ICT-service.
4. Het verstrekken van autorisaties voor beheerders van B/CICT vindt plaats op grond van de toegekende rol aan een medewerker en het daaraan gekoppelde autorisatieprofiel.
5. Toegangsrechten, toegekend aan beheerders die langer dan twee weken onaangekondigd niet gebruikt worden, worden verwijderd.
6. Bij het verstrekken van rechten aan beheerders wordt apart toezicht gehouden door medewerkers werkzaam in het proces monitoren beveiligingsinstellingen.

Richtlijn

EP B/CICT R-5	*Bij de uitvoering van werkzaamheden in het exploitatieproces dienen informatiebeveiligingsregels in acht te worden genomen.*

Risicoafweging

Het risico bestaat dat ondanks algemene maatregelen van logische en fysieke toegangsbeveiliging door middel van onzorgvuldige uitvoering van exploitatiewerkzaamheden de informatiebeveiliging van *ICT-Service*s en gegevens bewust of onbewust voor korte of langere termijn negatief wordt beïnvloed en zo de *informatiebeveiliging* van de Belastingdienst in gevaar brengt.

Norm

EP B/CICT N-5-1	Remote support en remote beheer door leveranciers en eigen medewerkers kan, in verband met de hieraan verbonden risico's, alleen worden uitgevoerd indien aanvullende *informatiebeveiligingsmaatregelen* zijn getroffen.

Maatregelen

1. Ten behoeve van remote support en/of beheer worden alleen die verbindingen en toegangsroutes hiervoor open gesteld die door O&B expliciet voor dit doel zijn aangewezen of ontworpen.
2. Indien bij remote support door leveranciers gebruik gemaakt wordt van mutatiebevoegdheden, wordt door eigen medewerkers meegekeken.

300939 0085

3. Het initiatief van het maken van een verbinding naar leveranciers ligt altijd bij B/CICT. De verbinding tussen leverancier en B/CICT geldt slechts voor een beperkte tijdperiode, n.l. zolang als de storingsafhandeling duurt.
4. De vastlegging van de beheerhandelingen bij remote support bevat altijd een verwijzing naar de incident registratie.

Norm

EP N-5-2 B/CICT	Voor het gebruik van netwerkdiagnose-apparatuur/-software (sniffers) gelden speciale beheerprocedures i.v.m. het risico van ontsluiting van (zeer) *vertrouwelijke gegevens*

Maatregelen

1. Door de proceseigenaar Exploitatie wordt een registratie bijgehouden van netwerkdiagnose-apparatuur/-software.
2. Mobiele netwerkdiagnose-apparatuur/ -software (sniffers) moet centraal in een afgesloten kast bewaard worden met een eenduidige regeling voor het sleutelbeheer.
3. Voor het gebruik van netwerkdiagnose-apparatuur/-software wordt vooraf schriftelijk toestemming verleend door de proceseigenaar Exploitatie.

300939 0085

2.2.7 Resource management

Richtlijn RM R-1

Norm RM N-1-1

- ***Vervallen bij RM proces, opgenomen onder POO N-2-1 en POO N-2-2 (6)***

Norm RM N-1-2

- ***Vervallen bij het RM proces, opgenomen onder POO N-2-2.***

Richtlijn

RM R-2 B/CICT	*Bij uitbesteding van werkzaamheden dient met de interne leverancier zodanige afspraken t.a.v. informatiebeveiliging te worden gemaakt dat het Basis Beveiligings Niveau niet wordt aangetast.*

Risicoafweging

Het niet maken en vastleggen van afspraken op het gebied van *informatiebeveiliging* bij uitbesteding van (onderdelen van) taken van B/CICT aan derden (in dit geval met name partners binnen de Belastingdienst), waarbij het HIB B/CICT uitgangspunt is, kan leiden tot ongewenste negatieve gevolgen voor het *Basis Beveiligings Niveau*.

Norm

RM N-2-1 B/CICT	Indien werkzaamheden worden uitbesteed voldoen de leveranciers van de (onderdelen van) taken op het gebied van informatiebeveiliging aan de normen zoals deze in dit document zijn opgenomen.

Maatregelen

1. In de SNO wordt bij het uitbesteden van werkzaamheden wordt standaard een eis opgenomen inzake het controlerecht, waarbij:
   1.1. leverancier eenmaal per jaar zal zorgen voor een mededeling van een onafhankelijke deskundige, waaruit blijkt dat leverancier zowel in opzet, bestaan als werking gedurende het jaar voldoet aan de afspraken die worden overeengekomen op het gebied van vertrouwelijkheid, *integriteit* en beschikbaarheid. Deze afspraken mogen geen afbreuk doen aan het Basis Beveiligings Niveau, zoals in dit document is verwoord.
   1.2. B/CICT gerechtigd is de hiervoor bedoelde mededelingen te laten reviewen.
   1.3. B/CICT gerechtigd is tussentijds een kwaliteitstoetsing ten aanzien van de verlening van *Services* door leverancier op basis van de overeenkomst alsmede ten aanzien van vertrouwelijkheid, *integriteit* en beschikbaarheid van de door leverancier ter beschikking gestelde *Services* door een onafhankelijke deskundige te laten uitvoeren;
   1.4. leverancier zich bereid verklaart mee te werken aan een dergelijke voorgenomen toetsing en de door de deskundige aangegeven aanbevelingen ter verbeteringen, voor zover redelijkerwijze mogelijk, uit te voeren.
2. Er wordt regelmatig met de leverancier van de uitbestede taak overlegd over de resultaten van de dienstverlening die in een SNO rapportage worden vastgelegd.

300939 0085

Richtlijn

RM R-3 B/CICT	*Indien, ondanks alle risicobeheersingsmaatregelen genoemd in het basis-beveiligingsniveau, er onverhoopt toch calamiteiten optreden dienen deze beheerst te worden afgehandeld.*

Risicoafweging

Het is belangrijk om de voortgang van de bedrijfsvoering onder vrijwel alle omstandigheden te waarborgen. In het basisbeveiligingsniveau is een groot aantal maatregelen genoemd om te anticiperen op mogelijke risico's. Er kunnen zich toch *calamiteiten* voordoen die grote inbreuk kunnen hebben op de bedrijfsvoering. Om de bedrijfsvoering zo veel mogelijk toch doorgang te laten vinden worden hieronder een aantal bijzondere maatregelen genoemd. Voor de maatregelen op het gebied van *calamiteiten* rond informatiesystemen wordt ook verwezen naar POO R-3.

Norm

RM N-3-1 B/CICT	De continuïteit van de bedrijfsvoering van B/CICT is gewaarborgd.

Maatregelen

1. Door RM wordt een lijst met onmisbare functie's – rollen opgesteld die voor de bedrijfsvoering onontbeerlijk zijn. Aan personen die deze functie's – rollen uitvoeren wordt speciale aandacht besteed teneinde maximaal van de kennis en ervaring van deze medewerkers gebruik te maken.
2. De kennis en ervaring van onmisbare medewerkers wordt zo veel mogelijk geborgd door deze kennis over meerdere medewerkers te verdelen en/of vervanging te regelen.
3. In het SNO met B/CFD worden afspraken opgenomen over het Bedrijfshulpverleningsplan en het ontruimingsplan.

Richtlijn

RM R-4 B/CICT	*Gegevens van Belastingplichtigen, vertrouwelijke personeelsgegevens en vertrouwlijke gegevens met betrekking tot de bedrijfsvoering dienen te worden afgeschermd voor onbevoegden.*

Risicoafweging

Het mag niet voorkomen dat gegevens van Belastingplichtigen, vertrouwelijke personeelsgegevens en *vertrouwelijke gegevens* met betrekking tot de bedrijfsvoering (samengevat onder de term *vertrouwelijke gegevens*) door onbevoegden kunnen worden ingezien of misbruikt. Daarom dienen er speciale maatregelen te worden genomen om deze gegevens te beschermen. Behalve de maatregelen tot functiescheiding en authenticatie en autorisatie in de door de werknemers gebruikte automatiseringssystemen dienen er ook andere eisen te worden gesteld aan mensen, gebouwen en middelen.

Norm

RM N-4-1 B/CICT	Gebouwen waarin medewerkers van B/CICT hun werkzaamheden uitvoeren zijn beperkt toegankelijk.

Maatregelen

1. Met de B/CFD wordt met betrekking tot het beheer van gebouwen en de beveiliging daarvan een SNO afgesloten waarin de volgende afspraken worden uitgewerkt:

300939 0085

1.1. Behalve de entree tot de gebouwen waarin medewerkers van B/CICT hun werkzaamheden uitvoeren zijn alle ruimten binnen de gebouwen niet openbaar.
1.2. Publieke ruimten in de gebouwen in gebruik bij B/CICT (bedrijfsrestaurants, bibliotheek, vergaderzalen) zijn toegankelijk voor medewerkers van B/CICT en bezoekers.
1.3. Alle overige ruimten in gebouwen in gebruik bij B/CICT, niet zijnde openbare of publieke ruimten, worden gekwalificeerd als dienstruimten (met uitzondering van aan te wijzen *kritische ruimten*).
1.4. Alle medewerkers van B/CICT hebben toegang tot alle dienstruimten in alle gebouwen in gebruik bij B/CICT.
1.5. Op basis van een analyse van de risico's ten aanzien van de aard van de werkzaamheden en de mogelijke toegang tot *vertrouwelijke gegevens* worden door de beveiligingscoördinator ruimten in gebruik bij B/CICT als *kritische ruimten* aangewezen.

2. Toegang tot de bovenbeschreven ruimten geschiedt d.m.v. een toegangspas die toegangspoorten bedienen. Op deze toegangsbeveiliging wordt door B/CFD toegezien.
3. Fysieke toegang tot gebouwen wordt geregeld door een autorisatieprofiel wat gekoppeld is aan een *procesrol*.
4. Bezoekers (= iedereen die niet door het management van B/CICT is aangesteld of tot tijdelijk medewerker is benoemd) wordt alleen onder begeleiding toegang verleend. Hiertoe worden bezoekers vooraf aangemeld en geregistreerd, waarna ze bij de ingang van het gebouw worden afgehaald door (of namens) degene onder wiens verantwoordelijkheid de bezoeker in de gebouwen van B/CICT verblijft.
5. Medewerkers worden alleen op basis van hun directe werkzaamheden met behulp van de toegangspas toegelaten tot de hierboven beschreven ruimten.
6. Het aanvragen en het verlenen van toegangsrechten wordt uitsluitend afgehandeld door middel van één geautomatiseerde procedure.
7. De afhandeling van het verkrijgen van de toegangspas (incl. diefstal, verlies, vermissing) geschiedt op de door B/CFD voorgeschreven wijze.
8. Bij vermissing of verlies van de belastingdienstpas door een individuele medewerker wordt deze melding door het verantwoordelijk management afgehandeld op basis van een vastgestelde procedure.
9. Medewerkers van en bezoekers aan B/CICT dragen hun pas zichtbaar, waarop door het management wordt toegezien.

Richtlijn

RM R-5 B/CICT	*Aan het personeel worden specifieke eisen gesteld op het gebied van integriteit en omgang met vertrouwelijke gegevens.*

Risicoafweging

Personeel is een belangrijke factor voor informatiebeveiliging en *integriteit*. Dit geldt zowel voor de wijze waarop formeel (via voorschriften) met het personeel wordt omgegaan als voor de wijze waarop het personeel omgaat met informatiebeveiliging en *integriteit*. De eisen met betrekking tot informatiebeveiliging en *integriteit* worden bepaald door de taak of functie van de medewerker. Voor intern personeel is het Algemeen Rijksambtenarenreglement (ARAR), de Ambtenarenwet en het Reglement Personeelsvoorschriften Belastingdienst (RPVB) geldend, die automatisch een aantal integriteitsregels en sancties geven. Voor extern personeel zijn aanvullende normen gesteld, die in de mantelovereenkomst met de leveranciers van extern personeel worden opgenomen.

300939 0085

Norm

RM N-5-1 B/CICT	Bij aanstelling, benoeming en tewerkstelling van een medewerker (in- en extern) wordt de *integriteit* van de medewerker beoordeeld.

Maatregelen

1. Voorafgaande aan de aanstelling, benoeming en de tewerkstelling van een medewerker wordt vastgesteld of aan de wettelijke vereisten ten aanzien van identificatie is voldaan.
2. Voorafgaande aan de aanstelling, benoeming en de tewerkstelling van een medewerker wordt vastgesteld of voor de betreffende functie speciale eisen m.b.t. *integriteit* van toepassing zijn.
3. Een kopie van het originele identiteitsbewijs wordt opgenomen in het personeelsdossier.
4. Verklaring omtrent gedrag wordt opgenomen in het personeelsdossier.
5. Het management neemt bij iedere nieuwe medewerker behorende tot het interne personeel de ambtseed of de belofte af. De schriftelijke verklaring van de ambtseed/belofte wordt door de nieuwe medewerker als door het management ondertekend en opgenomen in het personeelsdossier.

Norm

RM N-5-2 B/CICT	De medewerkers zijn op de hoogte van de geldende beveiligings- en integriteitsregels.

Maatregelen

1. de medewerker word geïnformeerd, zowel bij indiensttreding als periodiek, over de geldende informatiebeveiligings- en integriteitregels en over de noodzaak ervan.
2. De onderwerpen informatiebeveiliging en *integriteit* zijn periodiek onderdeel van het reguliere afdelings- en werkoverleg.
3. Media als bulletins en nieuwsbrieven worden gebruikt om toevoegingen en/of wijzigingen in de regels of concrete noemenswaardige gevallen die zich hebben voorgedaan onder de aandacht van het personeel te brengen
4. In voortgangsgesprekken en beoordelingen wordt informatiebeveiliging en *integriteit* als aandachtsgebied meegenomen, het resultaat van de beoordeling wordt vastgelegd op het RGL-beoordelingsformulier. Het RGL-beoordelingsformulier wordt opgenomen in het personeelsdossier.
5. Daartoe aangewezen medewerkers volgen de belastingdienstbreed ontwikkelde en beschikbaar gestelde trainings- en opleidingsprogramma's en/of modules op het gebied van informatiebeveiliging en *integriteit*.

Norm

RM N-5-3 B/CICT	*Gegevens van Belastingplichtigen, vertrouwelijke personeelsgegevens en vertrouwelijke gegevens met betrekking tot de bedrijfsvoering mogen alleen worden ingezien door bevoegden.*

Maatregelen

1. Vertrouwelijke gegevens worden afgeschermd van onbevoegden.
2. Na gebruik van documenten waarop vertrouwelijke gegevens staan vermeld worden deze opgeborgen in een afgesloten kast of bureau.

Norm N-5-4

- **Norm is opgenomen onder RM N-7-1**

300939 0085

Norm

RM N-5-5 B/CICT	*Medewerkers zijn zich er van bewust dat hun doen en laten het gezicht van de Belastingdienst bepaalt en dat hun integriteit boven iedere twijfel verheven is.*

Maatregelen

1. medewerkers mogen geen nevenwerkzaamheden verrichten – betaald of onbetaald – die leiden of zouden kunnen leiden tot (de schijn van):
   1.1. Belangenverstrengeling;
   1.2. schade aan het aanzien van de dienst of van het ambt;
   1.3. onvoldoende beschikbaarheid voor de functie.
2. Medewerkers mogen geen aandelenportefeuille in bedrijven waarmee B/CICT zaken doet bezitten, indien dit in het functioneren rechtstreeks een belemmering vormt of waardoor de medewerker met voorkennis kan handelen.
3. Nevenwerkzaamheden die conform het RPVB moeten worden gemeld, worden gemeld bij en getoetst door de leidinggevende die van deze melding een notitie maakt in het personeelsdossier,
4. De medewerkers van B/CICT mogen geen geschenken accepteren, waaronder begrepen uitnodigingen van derden om een bijeenkomst (waaronder niet begrepen educatieve bijeenkomsten) bij te wonen. Van de poging om een geschenk aan te bieden dient de leidinggevende op de hoogte te worden gebracht. Deze maakt hiervan een melding ‘integriteitincident’.
   Er is binnen B/CICT een vertrouwenspersoon *integriteit* waarop de medewerkers een beroep kunnen doen.
5. Medewerkers in de functie Contractbewaker, ICT-productbeheerder, ICT-servicebeheerder en Hoofd Crediteurenadministratie dienen, vanwege de directe contacten met derde partijen, eens in de vijf jaar van functie/rol te wisselen teneinde een te nauwe relatie met de derde partij te voorkomen. Deze functie/rol-wisseling kan bestaan in roulatie t.a.v. de derde partijen waarmee in de volgende periode van vijf jaar relaties worden onderhouden.

Norm

RM N-5-6 B/CICT	*Het gebruik van de ter beschikking gestelde bedrijfsmiddelen is eenduidig gedefinieerd en toegepast.*

Maatregelen

1. Middels een getekende verklaring die in het personeelsdossier wordt opgenomen wordt de werknemer aansprakelijk gesteld voor de aan hem/haar verstrekte bedrijfsmiddelen,
2. In de verklaring zijn de gedragsregels voor de aan hem/haar verstrekte bedijfsmiddelen opgenomen..
3. Er wordt geregistreerd welke medewerkers welke bedrijfsmiddelen onder zich hebben.
4. Het toekennen van wachtwoorden na blokkade of kwijtraken wordt alleen door daartoe aangewezen medewerkers van RM verricht.
5. De medewerker ondertekent een verklaring van goed gebruik voor de verkregen ontheffing.
6. De voorschriften zoals beschreven in de E-mail en internet conventies van de Belastingdienst voor het gebruik van e-mail en internetwerkplek worden nageleefd.
7. Er wordt toegezien op het juiste gebruik van de ter beschikking gestelde bedrijfsmiddelen.

Richtlijn R-6

Norm N-6-1

- **Vervallen bij RM en opgenomen onder POO N-4-1**

300939 0085

Norm N-6-2

- **Vervallen bij RM en opgenomen onder POO N-2-1**

Richtlijn

RM R-7 B/CICT	*Autorisatieprofielen die niet gekoppeld zijn aan een specifieke procesrol en aan een medewerker worden vermeden.*

Risicoafweging

Het niet koppelen van autorisatieprofielen aan *procesrol*len betekent dat bepaalde rollen ongecontroleerde bevoegdheden hebben waardoor ongewenste activiteiten kunnen worden uitgevoerd en hierdoor beveiligingsrisico's kunnen optreden. Ditzelfde geldt voor het niet koppelen van *procesrollen* aan medewerkers. Dit betekent dat bij het in- door- en uitstromen van medewerkers de koppelingen tussen autorisatieprofielen, *procesrollen* en medewerker actueel moet worden gehouden en mutaties gecontroleerd moeten plaatsvinden.

Norm

RM N-7-1 B/CICT	*Bij de in- door- en uitstroom van medewerkers dienen mutaties van procesrollen en daaraan gekoppelde autorisatieprofielen gecontroleerd plaats te vinden.*

Maatregelen

1. In het proces RM wordt bij in diensttreding en bij doorstroom een medewerker gekoppeld aan een functie en *procesrol* en de daaraan gekoppelde autorisatieprofielen voor toegang tot systemen én toegang tot gebouwen.
2. Bij doorstroom wordt tevens het bij de vorige functie en *procesrol* gekoppelde autorisatieprofiel ingetrokken.
3. Een exemplaar van de ingevulde checklist "Doorstroom medewerker" wordt ter controle achtergehouden in de administratie tot in ieder geval één jaar na doorstroom.
4. Bij vertrek bij B/CICT van een medewerker worden de volgende maatregelen uitgevoerd:
   4.1. Uiterlijk op de laatste werkdag worden alle bevoegdheden (logisch en fysiek) van de vertrekkende medewerker ingetrokken wat wordt vastgelegd op de checklist "Uitstroom Medewerker".
   4.2. Aan de Belastingdienst toebehorende artikelen (bijvoorbeeld geleende IT-apparatuur, gegevensdragers, documentatie, passen, sleutels, mobiele telefoon, et cetera) die volgens de registratie verstrekte bedrijfsmiddelen zijn uitgereikt aan de vertrekkende medewerker worden ingetrokken uiterlijk op de laatste werkdag wat wordt vastgelegd op de checklist "Uitstroom Medewerker" en in de registratie verstrekte bedrijfsmiddelen.
   4.3. Een exemplaar van de ingevulde checklist "Uitstroom Medewerker" wordt ter controle achtergehouden in de eenheidsadministratie tot in ieder geval één jaar na uitstroom.
   4.4. De volledigheid en juistheid van verstrekte en ingenomen autorisaties en bedrijfsmiddelen wordt periodiek gecontroleerd.
5. Bij onvrijwillig ontslag wordt geïnventariseerd welke eventuele risico's als gevolg van het vertrek van een medewerker worden gelopen en worden treffende passende maatregelen om deze risico's te beperken.
6. In het proces RM wordt het geheel van functie, (proces)rolbeschrijving, het daarvoor benodigde autorisatieprofiel, en de daaraan gekoppelde medewerker beheerd.

3 Bijlage 1: Begrippenlijst

Begrip	Definitie
Acceptatie- testomgeving	De omgeving, die gebruikt wordt voor acceptatie en certificatie testen en waarin gebruikers mogen werken met niet-gecertificeerde applicatie-componenten.
Applicatie	Zie: Applicatief ICT product
Applicatief ICT-product	Een applicatief ICT-product is: - een (ongeparametriseerd) softwaresysteem voor de eindgebruiker inclusief documentatie, etc. welke bij inzet in een organisatie dient als een gegevensverwerkend informatiesysteem voor de ondersteuning van de processen van de klant **of** - een applicatie voor de eindgebruiker in te zetten voor de uitvoering van een specifieke taak van een medewerker (power point, excel, fotoshop). - software met een specifiek doel op het gebied van eindgebruikerscommunicatie (bijv. t.b.v intranet).
Basis Beveiligings Niveau	Het niveau van informatiebeveiliging dat bij B/CICT wordt bereikt door het implementeren en toepassen van de basismaatregelenset zoals geformuleerd in dit document (HIB B/CICT).
Bestandsmanipulatie	Van bestandsmanipulatie is sprake als delen van het invoerbestand worden geparkeerd om de productie doorgang te laten vinden, danwel bestanden worden teruggezet of gereconstrueerd. De inhoud van klantgegevens is onveranderd, er dient verantwoording over volledigheid afgelegd te worden. Onder bestandsmanipulaties worden legitieme niet voorziene bewerkingen op data in het proces Exploitatie bedoeld. Legitieme voorziene bewerkingen, die met behulp van de ICT – service worden uitgevoerd – worden niet hiertoe gerekend.
Beveiligingscoördinator	Ook wel ACO (Argi Coördinator)
Beveiligingsincident	Het manifest worden van een beveiligingsrisico m.b.t. een *ICT-Service* en/of de omgeving als gevolg van: - een overtreding van informatiebeveiligingsregel, bijv. onbevoegde toegang tot *ICT-componen*ten of omgeving; - ongebruikelijke (bevoegde) handelingen van beheerders met hoge systeemrechten; - een (vermoeden van) geschonden technische *integriteit of vertrouwelijkheid* van gegevens; - een incidentele *bestandsmanipulatie*; - vermiste of gestolen *TIS-componenten*. - Verstoringen in de fysieke ruimte en/of stroomvoorziening
Beveiligingsinstellingen	In (ICT-)services kunnen in veel gevallen functionaliteiten, die invloed hebben op informatiebeveiliging geactiveerd of uitgeschakeld

300939 0085

Begrip	Definitie
	worden door het opgeven van parameterwaarden
Beveiligingsniveau	Het samenhangend geheel van *informatiebeveiligingsmaatregelen* van een gedefinieerd object.
Beveiligingsrisico	Gesignaleerde afwijkingen van gewenst gebruik en status van *ICT-component*en en hun omgeving, die het afgesproken niveau van beveiliging negatief beïnvloeden.
Buitengewoon voorval	Een buitengewoon voorval of incident is een (mogelijke) inbreuk of een poging tot inbreuk op de ambtelijke integriteit of de beveiliging (waaronder de informatiebeveiliging), algemeen of door menselijk handelen. Ook de gesignaleerde risico's op het gebied van de integriteit of de (informatie)beveiliging vallen onder deze definitie.
Calamiteit	Een incident die, indien niet opgelost, na verloop van tijd een zodanig effect heeft dat de productievoortgang voor de Belastingdienst gevaar loopt.
Dienst	Een dienst is een specifieke activiteit uitgevoerd door een persoon. In voorkomende gevallen geschiedt de uitvoering van de activiteit op verzoek van een persoon, bij noodzakelijke periodieke uitvoering op basis van gemaakte afspraak.
Functioneel Beheer(der)	De beheertaken benodigd voor het in stand houden van de met de klant-opdrachtgever overeengekomen goede werking van de functionaliteit van een *ICT-Service*.
Gegevenseigenaar	Degene die uiteindelijk verantwoordelijk is voor de integriteit van de data: - De gegevens behorende bij de massale processen is B/CA; - De configuratiegegevens (ICT-)services is proceseigenaar Exploitatie; - voor de overige gegevens geldt dat de voorzitter van de regio waar de gegevens zijn aangemaakt, eigenaar is. -
Gegevensmanipulatie	Van gegevensmanipulatie is sprake als gegevens van de Belastingdienst inhoudelijk worden aangepast. er dient te allen tijde verantwoording over de integriteit van de gegevens afgelegd te worden.
ICT-component	Een ICT-product wat onderdeel uitmaakt van de *ICT-service*.
ICT-product	Een ICT-product is een product specifiek op het terrein van de Informatie- en Communicatie Technologie (hardware, software of eventueel een combinatie van beide).
(ICT-)service	Een service wordt herkend als een product die de Belastingdienstprocessen ondersteund. Een service wordt altijd vergezeld van een document waarin de afspraken worden vermeld

300939 0085

Begrip	Definitie
	die B/CICT maakt met de klant over de service. Dit document wordt een service niveau overeenkomst (SNO) genoemd. Deze afspraken hebben betrekking op de diensten die B/CICT levert om het klantproces te ondersteunen. Een ICT-service is een service op het gebied van ICT waarbij door middel van de inzet en levering van applicatieve en infrastructurele ICT-producten en bijbehorende diensten een gespecificeerde behoefte van (potentiële) interne klanten wordt ingevuld. De diensten kunnen algemeen van aard zijn of richten zich op de betreffende ICT-producten. Een ICT – service kan altijd alleen worden ontworpen in samenhang met de daarbij te leveren diensten om het ICT – product, wat een onderdeel vormt van de ICT – service, te laten werken.
Informatiebeveiliging	Het door risico-inschatting verkregen stelsel van richtlijnen en normen gericht op het voorkomen van bedreigingen die de integriteit van data, informatie en organisatie in gevaar kunnen brengen.
Informatiebeveiligingsincident	Het bij de eindgebruiker opgetreden incidenten welke de integriteit van data, informatie en organisatie in gevaar kunnen brengen.
Informatiebeveiligingsmaatregelen	Maatregelen die er op gericht zijn te voldoen aan de normen op het gebied vertrouwelijkheid, *integriteit* en beschikbaarheid van gegevens en *ICT-Service*s.
Informatiebeveiligingsverstoringen	Het door het proces Monitoren opgespoorde afwijkingen van afgesproken drempelwaarden zoals vastgelegd in het stelsel van richtlijnen en normen gericht op het voorkomen van bedreigingen die de integriteit van data, informatie en organisatie in gevaar kunnen brengen.
Informatiesysteem	Een informatiesysteem is een geparametriseerd en ingericht softwaresysteem (*applicatief ICT-product*) welke dient voor de ondersteuning van de processen van de klant. Parameterisering en inrichting van een softwaresysteem betekent dat proces, organisatie, mensen en systeem bij elkaar worden gebracht (inregelen van bedrijfsconcepten, vastlegging besturing van een organisatie, richtlijnen voor gebruik, functies medewerkers koppelen).
Infrastructureel ICT product	Een infrastructureel ICT-product is een randvoorwaardelijk ICT-product voor de werking van applicatieve ICT-producten. Tot de infrastructurele ICT-producten behoren alle ICT-product- en welke niet vallen onder de definitie van *applicatief ICT-product*. Tot de infrastructurele producten behoren dus hardware, middelware, operating systems, brokers, etc.,etc.
Inkoopproduct	Een inkoopproduct is een product wat ingekocht wordt bij derden.
Integriteit (gegevens)	De mate waarin gegevens een afbeelding van de werkelijkheid zijn (juistheid, volledigheid en tijdigheid). Bij B/CICT gaat het om de

Begrip	Definitie
	technische integriteit ofwel het ongeschonden blijven van de gegevens.
Integriteit (medewerkers)	Het begrip integriteit wordt ook gebruikt in de betekenis van onkreukbaarheid, moreel hoogstaand gedrag van medewerkers
Integriteitsincident	Een incident vanwege het niet nakomen van de beveiligings- en integriteitsregels die zijn opgesteld ten behoeve van personeel en organisatie.
Kritische ruimte	Ruimten waar vertrouwelijke gegevens (classificering departementaal vertrouwelijk) van de Belastingdienst worden verwerkt, opgeslagen of kunnen worden ingezien. Deze ruimten hebben een zonering op niveau D. Het is mogelijk deze zonering te specificeren al naar gelang het risico van manipulatie en/of misbruik van gegevens in deze ruimten toeneemt.
Labomgeving	De omgeving, die gebruikt wordt voor infrastructuurontwikkeling, -bouwtesten en innovatie en waarin gebruikers met niet-gecertificeerde *ICT-componen*ten mogen werken.
Onbedoelde of ongeautoriseerde ontsluiting van of inzage in gegevens	Onbedoelde ontsluiting van of inzage in gegevens kan optreden door onbewust foutieve handelingen in combinatie met onvoldoende informatiebeveiliging. Ongeautoriseerde ontsluiting van of inzage in gegevens treedt op bij bewuste handelingen met het oogmerk door te dringen tot vertrouwelijke gegevens.
Ontwikkelomgeving	De omgeving, die gebruikt wordt voor applicatieontwikkeling en applicatiebouwtesten en waarin gebruikers mogen werken met niet-gecertificeerde applicatie-componenten.
Operationeel Beheer	De beheertaken die nodig zijn om na installatie in de *Productieomgeving* de *ICT-Service* operationeel te houden conform de afspraken die hierover in het SNO zijn gemaakt.
Platform	Een platform is de combinatie van een tweetal infrastructurele ICT-producten namelijk hardware en operating system tezamen randvoorwaardelijk voor de werking van applicatieve ICT-producten.
Privacy-gevoelige informatie	Informatie over personen die, in de zin van de wet op de bescherming persoonsgegevens, niet mag worden verspreid, gebruikt of verwerkt zonder aanvullende maatregelen.
Procesrol	De in het project HIL gedefinieerde Bedrijfsrol.
Productiegegevens	Gegevens (data) die worden gerealiseerd in de *Productieomgeving*.
Productieomgeving	De omgeving, die gebruikt wordt voor het exploiteren van *ICT-Service*s en waarin gebruikers uitsluitend mogen werken met gecertificeerde *ICT-componen*ten.
Programmatuurbeheersysteem	Het *Programmatuurbeheersysteem* is een informatiesysteem dat programmaversies in al hun stadia van ontwikkeling, onderhoud en

Begrip	Definitie
	productie registreert en bewaart, deze aan bevoegden ter beschikking stelt en de overdracht tussen omgevingen regelt.
Risico	De kans dat een bepaalde dreiging zich voordoet vermenigvuldigt met de schade die zich voordoet.
Security Specialist / officer / Medewerker monitoring beveiliging / beveiligingscoördinator	De medewerkers die de juiste en tijdige verwerking van autorisatieaanvragen in de systemen, het onderhoud van beveiligingstructuren en de dagelijkse bewaking van de goede werking van de toegangsregels verzorgen. Deze medewerkers maken onderdeel uit van het operationeel beheer van *ICT-componen*ten. De beveiligingsrollen zijn onderwerp van discussie op Belastingdienst niveau. Een samenhangend beveiligingsfunctiegebouw moet (nog) ontstaan.
Service	Een service is het resultaat van een benoemde vorm van dienstverlening waarbij een leverancier door middel van de inzet en levering van producten en bijbehorende diensten, in operationele zin een gespecificeerde behoefte van (potentiele) externe clientele invult. De benoemde vorm van dienstverlening wordt afgenomen tegen een vastgestelde prijs en tegen een vastgesteld kwaliteitsniveau.
Serviceontwerp	Een *Serviceontwerp* is het inhoudelijk kader waarbinnen de uiteindelijke levering van de *ICT-Service* kan plaatsvinden.
Vertrouwelijke gegevens	Vertrouwelijke gegevens zijn: - gegevens traceerbaar naar natuurlijke- cq. rechtspersonen; - fiscale gegevens; - configuratiegegevens *ICT-componen*ten van de infrastructuur.

4 Bijlage 2: Overzicht wijzigingen ten opzichte van het HIB B/CICT 2007

In onderstaande tabel is weergegeven wat de wijzigingen zijn in voorliggend HIB B/CICT ten opzichte van de versie uit 2007 (HIB B/CICT 2007).

#	Was	Is in HIB 2009: toelichting (gewijzigd in HIB B/CICT 2009)
1.	Algemeen	Bullets van de maatregelen zijn genummerd.
2.	HS 1.	Kleinere aanpassingen als gevolg van de organisatiewijziging 2008.
3.	1.2. Doel	Overzicht samenhang processen en normatiek beveiliging opgenomen.
4.	ALG N-1-1	POO N-2-1: Norm gaat over procesinrichting organisatie waarin samenhang van informatiebeveiligingsbeleid in organisatie, proces, personeel en techniek wordt geregeld, inclusief procesrollen en autorisaties.
5.	ALG N-1-2	ALG N-1-1.
6.	ALG N-2-1	Maatregel 1: aangevuld met call-afhandelingsproces. Maatregel 3 en 4: 'informatiebeveiligingsplan' verwijderd.
7.	POO algemeen	De normatiek op het gebied van beveiligen is bij het proces POO uitgebreid. Dit komt omdat in dit proces o.a. randvoorwaarden worden geschapen waarbinnen andere processen werken. Het gaat hierbij m.n. om normatiek die in de ontwerpfase van de processen meegenomen wordt. Ook is het gedeelte van RM-ICT waarbinnen autorisatiebeheer plaatsvindt onder het POO proces opgeschreven. In het vorige handboek waren onder het proces RM maatregelen opgenomen die onder POO hoorden. Ook is regelgeving m.b.t. de WBP aangescherpt.
8.	POO N-1-1	Maatregel 1: toegevoegd 'de normen procesbeheersing'.
9.	POO N-1-2	Maatregel 1 en 2: terminologie aangepast aan gewijzigde organisatie. Maatregel 3: de afhandeling van incidenten als gevolg van menselijk handelen toegicht op afhandeling hiervan. Maatregel 4: verantwoordelijkheden scherper benoemd.
10.	POO N-1-3	In deze norm wordt nu via de maatregel verwezen naar het 'crisismanagementplan'. Hiermee is overtollige tekst verwijderd.
11.	POO N-1-4	In de norm is de tekst aangescherpt. Termen 'bedreigingen, agressie en geweld' zijn vervangen door 'buitengewone voorvallen' een term die beter aansluit bij het karakter van de bedrijfsvoering binnen B/CICT.
12.	POO N-1-5	Toegevoegde norm die de 'act' van beleid op het gebied van *integriteit* en beveiliging regelt.
13.	POO N-2-2	Was RM N-1-2, i.v.m. koppeling autorisatieprofiel aan procesrol is dit opgenomen onder het POO proces.
14.	POO N-3-1	Was voor een groot gedeelte RM N-3-1.
15.	POO R-4 en POO N-4-1	Was RM R-6 en RM N-6-1, naar POO proces.
16.	AM N-1-1	Maatregel 3: toegevoegd. Verscherpt de verantwoordelijkheid van de opdrachtgever om na te denken over gewenste logging i.v.m. integriteitsonderzoeken.
17.	AM N-1-2	Maatregel 3: toegevoegd. Middels deze maatregel is geborgd dat bij het Ontwerp de gemaakte afspraken over beveiligingsrisico's worden meegenomen. Maatregel 5: toegevoegd. Met deze maatregel is geborgd dat de opdrachtgever kennis heeft genomen van het VBI en VBA en een afweging heeft gemaakt.
18.	AM N-1-3	Tekstuele aanpassing 'BasisBeveiligingsNiveau' is vervangen door 'beveiligingsniveau zoals in het HIB B/CICT is vastgelegd'.
19.	Arch N-1-1	Maatregel 2: toegevoegd. Hierin wordt expliciet verwezen naar de domeinarchitectuur Beveiliging.

300939 0085

		Maatregel 4: tekst versimpeld.
20.	Arch N-1-2	Nieuwe norm die ingaat op architectuurcontrol op het gebied van beveiliging.

O&B algemeen

Het O&B proces begint in de versie 2009 met een richtlijn die voor het gehele proces geldt (R1 en N-1-1) over het gebruik van vertrouwelijke data). Vervolgens zijn richtlijnen en bijbehorende normatiek verdeeld naar risico's die op kunnen treden in het

- voortbrengingsproces (O): R2 (N-2-1 t/m N-2-4)
- het ICI proces R3 (N-3-1),
- het Beheerproces (B) R4 (N-4-1 t/m N-4-4).

In onderstaande tabel worden de normen toegelicht volgens het HIB B/CICT 2009

nr	RL/norm HIB 2009	Toelichting
21.	R-1	Deze richtlijn was in het HIB B/CICT 2007 norm N-2-1. Aangezien deze norm over het gehele O&B proces geldt is dit de eerst opgenomen richtlijn geworden.
22.	O&B N-1-1	Is aangescherpt op maatregelniveau waarbij controles op noodzakelijk gebruik van productiegegevens vooraf en achteraf zijn geborgd.
23.	O&B R-2	Was R-1. De tekst van de richtlijn is beperkt tot het 'voortbrengen'.
24.	O&B N-2-1	Was (delen van) N-1-1, N-1-3 Maatregel 1: toegevoegd om te borgen dat rekening wordt gehouden met de domeinarchitectuur. Maatregel 2: toegevoegd. Maatregel 3: was in het HIB 2007 maatregel 3 uit N-2-4. Maatregel 4: toegevoegd om te expliciteren dat testspecificaties in het ontwerp worden meegenomen. Maatregel 5: borgen het opnemen van aanwijzingen bij evt. noodzakelijk uit te voeren manipulaties. Maatregel 6: licentiegebruik buiten contractuele afspraken leidt tot risico's voor bedrijfsvoering
25.	O&B N-2-2	Geven aanwijzingen in de ontwerpfase voor uit te voeren monitoring, inclusief licentiegebruik
26.	O&B N-2-3	Aanwijzingen over groepsautorisaties moeten bij ontwerp worden meegenomen. Stonden in 07 bij EX N-4-1
27.	O&B N-2-4	Het expliciteren van het uitvoeren van testen op beveiligingsnormatiek.
28.	O&B R-3	Was N-2-2. Zie algemene toelichting voor het ICI proces is een separate richtlijn en norm opgenomen.
29.	O&B R-4	De aparte richtlijn en bijbehorende normatiek voor wat betreft beheer van de (ICT-) services, incl. licentiegebruik.
30.	O&B N-4-5	Norm aangaande handmatig wijzigen van gegevens en/of bestandsmanipulaties is aangescherpt. Inclusief uitwerking van de rol van de (ICT-)servicebeheerder.

#	Was	Is in HIB 2009: toelichting (gewijzigd in HIB B/CICT 2009)
31.	DM algemeen	Hoewel organisatorisch het daadwerkelijk verbinden met leveranciers verlegd is naar een ander organisatieonderdeel, in het proces DM blijft het stellen van de eisen op het gebied van beveiliging onverminderd van kracht.

300939 0085

32.	DM N-1-2	2.6 toegevoegd, borgt de kennisname van de leveranciers van het HIB B/CICT.
33.	EX N-1-1	Maatregel 2: aangevuld met toelichting.
34.	EX N-1-2	Termen als 'back-up en recovery' vervangen door dupliceermechanismen. Norm EX N-1-3 was N-3-6.
35.	EX N-1-3	Is EX N-1-4 geworden waarbij terminologie 'security violations' is vervangen door 'beveiligingsrisico's'. Maatregel 3: escalatiemogelijkheid naar Beveiligingscoördinatori toegevoegd.
36.	EX N-1-4	Is nu EX N-1-5. Maatregelen zijn aangescherpt en enkele toegevoegd.
37.	EX R-2 EX N-2-1	De term 'computerruimten' is vervangen door '*kritische ruimten*'.
38.	EX R-3	Term 'productiegegevens van klanten' vervangen door 'gegevens'. Tevens klopte de nummering in het HIB B/CICT 2007 niet. Is aangepast. Maatregelen zijn in enkele normen verscherpt. Ook zijn maatregelen i.v.m. WBP toegevoegd.
39.	EX N-4-1	Is in O&B N-2-3 opgenomen waar in het ontwerp rekening wordt gehouden met benodigde groepsautorisaties. In EX N-4-1 zijn de maatregelen aangaande toegangsrechten specifieker uitgewerkt.
40.	EX N-4-2	Maatregel 2 toegevoegd waarbij rekening wordt gehouden met de autorisatieprofielen van B/CA. Maatregel 3 toegevoegd inzake noodzakelijke wijzigingen in groepsautorisaties t.b.v. de *functioneel beheerder*.

In de normatiek en maatregelen van RM stonden in de versie HIB 2007 een aantal zaken die randvoorwaardelijk in het POO proces geregeld moeten worden. Zie ook toelichting bij POO. Het gaat hierbij met name dat in POO aan een procesrol autorisatieprofielen worden toegekend die zowel de logische als fysieke toegang regelt. Hiermee worden een aantal normen bij RM overbodig. Voor het proces RM is de oorspronkelijke nummering aangehouden i.v.m. de aansluiting op bestaande Interne Controle Programma's. Aangegeven is een verwijzing opgenomen waar de norm in deze versie nu is opgenomen.

Metagegevens

Documenteigenschappen

Filenaam	Gouden regels voor omgang met vertrouwelijke informatie
Laatste wijziging	14 Juli 2020
Huidige status	Definitief
Versienummer	2.1

Toelichting status

Concept:	Praatstuk voor onderlinge afstemming tussen auteurs (collegiale review).
Review:	In review bij Reviewers
Definitief:	Goedgekeurd door stakeholder/opdrachtgever of Vastgesteld in overleg.

Documenthistorie

Versie	Status	Datum	Omschrijving
0.01	Concept	4-7-2017	Initiële versie
0.1	Review	6-7-2017	Tien regels gedefinieerd. Openlijke publicatie op CP en fysiek op muur, ter review bij alle collega's DF&A
0.8	Concept	11-9-2017	Tientallen opmerkingen van collega's verwerkt
0.82	Review	14-9-2017	Versie ter review bij Persoonsgegevens (zie 'Reviewers' hieronder)
0.96	Concept	22-9-2017	Review verwerkt, versie ter voorlegging aan MT
1.0	Definitief	10-10-2017	Versie vastgesteld door MT
1.1	Definitief	5-2-2018	Lessons learned toegevoegd
1.2	Definitief	5-2-2019	GR1 aangepast n.a.v. IC-procedure, toelichting 'werkbaarheid' toegevoegd aan GR2, verder tekstuele verbeteringen
1.8	Concept	29-7-2019	Eerste verbeterslag n.a.v. groot onderhoud
2.0	Definitief	11-2-2020	Versie vastgesteld door MT
2.01	Concept	1-7-2020	Aanpassingen GR3 en GR4
2.02	Concept	8-7-2020	Aanpassing aan GR9
2.1	Definitief	14-7-2020	Versie vastgesteld door MT

Auteurs (werkgroep 'gouden regels')

Naam	Organisatie-onderdeel	Rol
Persoonsgegevens	DF&A	Persoonsgegevens
	DF&A	Data scientist
	DF&A	Business analist
	DF&A	Solution architect
	DF&A	Data-expert
	DF&A	Data-informatiespecialist
	DF&A	Analytical Programmer

Reviewers

Naam	Organisatie-onderdeel	Rol
Alle medewerkers	DF&A	Data scientist, functioneel beheerder, projectmanager, teamleider, etc.
Persoonsgegevens	Vaktechniek	Persoonsgegevens
	DF&A	Persoonsgegevens

Stakeholders

Naam	Organisatieonderdeel	Rol
Persoonsgegevens (namens MT DF&A)	DF&A	Persoonsgegevens

Tien gouden regels voor omgang met vertrouwelijke informatie

Gouden regel 1: Bij twijfel of uitzondering, bespreek het en vraag akkoord.

Als het noodzakelijk is om af te wijken van onderstaande gouden regels, vraag dan eerst formeel akkoord van je direct leidinggevende. De uitgevoerde handeling en het akkoord worden inclusief onderbouwing schriftelijk vastgelegd door Persoonsgegevens

Gouden regel 2: Gegevens opslaan.

Plaats vertrouwelijke gegevens alleen op expliciet door DF&A goedgekeurde locaties.

Gouden regel 3: Gegevens delen.

Deel vertrouwelijke gegevens alleen door middel van expliciet door DF&A goedgekeurde methodes.

Gouden regel 4: Interne en externe communicatie.

Neem geen vertrouwelijke gegevens op in producten (rapportages, presentaties, etc.) die toegankelijk zijn voor niet-bevoegde personen.

Gouden regel 5: Doelbinding.

Gebruik alleen gegevens die geoorloofd zijn voor de uitvoering van je werk.

Gouden regel 6: Dataminimalisatie.

Gebruik niet meer gegevens dan die noodzakelijk zijn voor de uitvoering van je werk.

Gouden regel 7: Persoonsgegevens raadplegen.

Het raadplegen van persoonsgegevens mag enkel een zakelijk doel hebben binnen de context van je onderzoek. Je mag geen gegevens van jezelf of je persoonlijke omgeving raadplegen (bijv. partner, familie, collega, huisgenoot, buren, dienstverlener, etc.). Tenzij dit expliciet uit de opdracht blijkt, mag je niet gericht zoeken naar specifieke bedrijven of personen met een vooraanstaande functie (bijv. VIPs, dienstverleners, bestuurders van beursgenoteerde bedrijven, etc.).

Gouden regel 8: Wachtwoorden.

Werk altijd met je eigen wachtwoord. Leen je wachtwoord(en) nooit uit en schrijf ze niet op. Neem geen wachtwoorden op in programmatuur.

Gouden regel 9: iBewustzijn.

Houd er rekening mee dat er zowel op kantoor als daarbuiten onbevoegden kunnen meeluisteren en –kijken met je werkzaamheden.

Gouden regel 10: Denk mee.

Ben actief en kritisch bezig met de gouden regels en spreek collega's aan als ze ervan afwijken.

Inleiding en definities

De tien gouden regels zijn door het MT van DF&A bekrachtigd als een organisatorische maatregel die enerzijds bewustzijn creëert bij medewerkers over do's en don'ts rondom omgang met vertrouwelijke gegevens, en anderzijds een veilige werkomgeving biedt waarin medewerkers hun werkzaamheden met vertrouwelijke gegevens met vertrouwen durven uit te voeren. Wijzigingen op de gouden regels zijn pas geldig als ze door het MT zijn geaccordeerd en vervolgens via de mail en weekstart zijn gecommuniceerd. Periodiek vinden er interne controles plaats om te beoordelen in hoeverre de gouden regels worden nageleefd.

Hieronder worden enkele belangrijke begrippen rondom de gouden regels op een rij gezet.

Vertrouwelijke gegevens. Onder vertrouwelijke gegevens vallen gegevens van klanten en medewerkers (bijv. bsn, naam, adres), fiscaal relevante gegevens (bijv. data uit aangiftes, gegevens die zijn aangeleverd door derden, gegevens van intermediairs) en strategische informatie (bijv. business rules, hitrates, risicoscores).

Proportionaliteitsbeginsel. Dit houdt in dat het doel van de verwerking van persoonsgegevens in verhouding moet staan tot de inbreuk op de privacy van de betrokkene. Dit betekent ook dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk. Daarnaast mogen persoonsgegevens alleen toegankelijk zijn voor diegenen die daartoe bevoegd zijn (zie hieronder).

Subsidiariteitsbeginsel. Dit houdt in dat het beoogde doel (dat voor de verwerking van persoonsgegevens is vastgesteld) op de minst ingrijpende manier en met de minst ingrijpende middelen moet worden bereikt. Op deze manier wordt de privacy van de betrokkenen zo min mogelijk geschaad.

Need-to-know principe. Dit houdt in dat je alleen toegang mag hebben tot gegevens die noodzakelijk zijn voor de uitvoering van je werkzaamheden.

Bevoegdheid. Je bent bevoegd om vertrouwelijke gegevens te verwerken als je die gegevens nodig hebt voor de uitvoering van je werk. Bevoegdheden voor gegevens en autorisaties voor afgeschermde locaties kun je aanvragen bij je direct leidinggevende.

Bevoegdheid bepalen. Welke collega's (binnen of buiten DF&A) bevoegd zijn om bepaalde gegevens te ontvangen, wordt bepaald door je direct leidinggevende. Dit wordt schriftelijk vastgelegd, bijvoorbeeld in een projectplan. Afstemming hierover met andere directies loopt altijd via het lijnmanagement.

Functionaris Gegevensbescherming (FG). De FG is geen medewerker van DF&A en geldt Belastingdienstbreed als kennisautoriteit en aanspreekpunt bij onduidelijkheden.

Links opnemen naar:

IBB: Integraal Beveiliging Belastingdienst
http://intranet.belastingdienst.nl/cso/files/2019/07/iBB-Concept-juni-2019.pdf

PUB: Personele Uitvoeringsbepalingen Belastingdienst
http://intranet.belastingdienst.nl/bcie/formulieren/formulieren-index/pub-rpvb/#connections4wpReload

Intranetpagina over integriteit
http://intranet.belastingdienst.nl/een-integere-belastingdienst/

Link naar cursus iBewustzijn

Gouden regel 1: Bij twijfel of uitzondering, bespreek het en vraag akkoord.

Als het noodzakelijk is om af te wijken van onderstaande gouden regels, vraag dan eerst formeel akkoord van je direct leidinggevende. De uitgevoerde handeling en het akkoord worden inclusief onderbouwing schriftelijk vastgelegd door Persoonsgegevens

Toelichting

Direct leidinggevende. Je direct leidinggevende kan (afhankelijk van je rol) een teamleider, MT-lid of directeur zijn. Een product manager of scrummaster is geen leidinggevende. Als je direct leidinggevende op vakantie is, dan is de vervanger (mits dit ook een leidinggevende is) bevoegd om een akkoord te geven.

Advies. Je direct leidinggevende moet advies inwinnen bij de Data Protectie Officer. Deze kan indien nodig advies inwinnen bij de Functionaris Gegevensbescherming (zie hieronder) en/of Vaktechniek Formeel Recht.

Vastlegging. Voor de medewerker is een akkoord per e-mail van de direct leidinggevende voldoende om de handeling uit te voeren. De leidinggevende zorgt ervoor de afspraken centraal en schriftelijk door de DPO worden vastgelegd, waarbij minimaal de beschrijving van de handeling, de betrokkenen, de motivatie en de termijn van de afspraak worden vastgelegd. Op deze manier is de DPO de enige die alle afspraken kan inzien. De medewerker is zelf verantwoordelijk voor het eventuele verlengen van de termijn.

Rol Data Protectie Officer DF&A. De DPO geeft geen akkoord, alleen (gevraagd of ongevraagd) advies. De DPO bewaakt dat afspraken en akkoorden die verschillende leidinggevenden geven, consistent zijn. De DPO is een kennisautoriteit op het (grijze) gebied van de gouden regels.

Praktijkvoorbeelden

- Als je op de universiteit of een bedrijvenbeurs een presentatie over DF&A gaat geven met uitleg over onze risicomodellen, zorg dan dat je slides eerst worden goedgekeurd door je direct leidinggevende. Voor het achteraf delen van de slides is eventueel apart goedkeuring nodig (zie ook gouden regel 4).
- Als het voor je project nodig is om vertrouwelijke gegevens op te slaan op een gedeelde omgeving die niet is goedgekeurd door gouden regel 2, zorg dan eerst dat je hiervoor toestemming krijgt van je direct leidinggevende. Maak ook afspraken hoe lang de gegevens op die locatie kunnen blijven staan.

Gouden regel 2: Gegevens opslaan.

Plaats vertrouwelijke gegevens alleen op expliciet door DF&A goedgekeurde locaties.

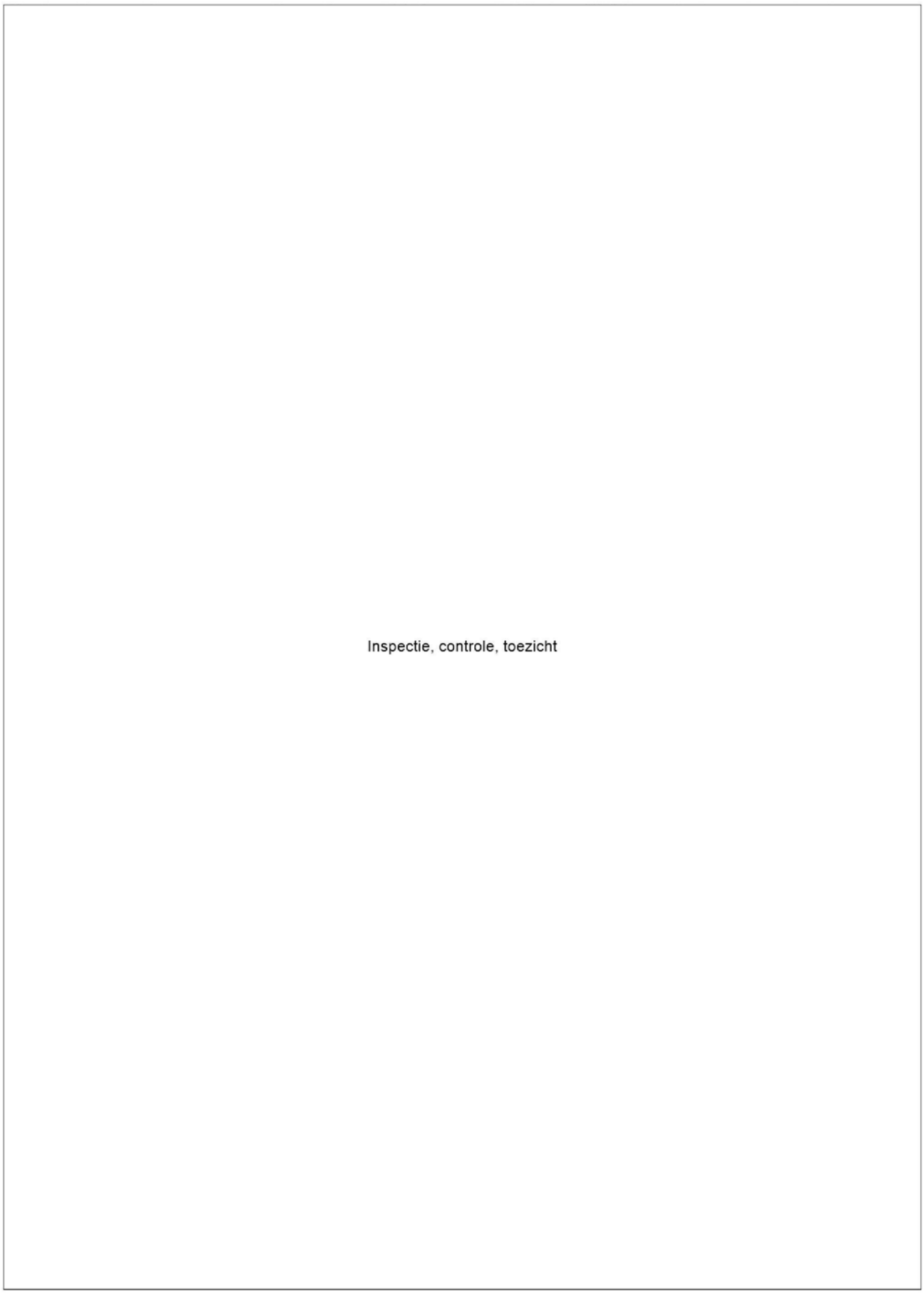
Toelichting

Inspectie, controle, toezicht

Praktijkvoorbeelden

- Het is niet toegestaan om vertrouwelijke gegevens te verplaatsen naar gegevensdragers buiten het domein van de Belastingdienst, bijvoorbeeld een externe of privélaptop, mobiele apparaten, externe harddisks of geheugensticks.
- Let op met printen, fotograferen of kopiëren van vertrouwelijke gegevens: op deze manier kunnen de gegevens makkelijker bij onbevoegden terechtkomen.

Gouden regel 3: Gegevens delen.



Inspectie, controle, toezicht

Praktijkvoorbeelden

- Wanneer je met externen bij DF&A samenwerkt, dan mag je geen vertrouwelijke gegevens mailen naar het extern e-mailadres van deze collega. Als de collega nog geen interne laptop heeft, dan zit er niets anders op dan hierop te wachten.
- Wees alert op het gebruik van de CC en BCC in e-mails, zeker als je via *reply-all* reageert op een e-mail die je hebt ontvangen.
- Het e-mailen van vertrouwelijke gegevens naar buitenlandse belastingdiensten of universiteiten is niet toegestaan. In navolging van gouden regel 1, kan je direct leidinggevende toestemming geven voor een uitzondering.
- Het delen van vertrouwelijke gegevens via berichtendiensten als WhatsApp, Signal, Telegram, etc. is ook niet toegestaan. Dit zijn onveilige kanalen voor het uitwisselen van fiscale informatie over een belastingplichtige of belastingschuldige.

Gouden regel 4: Interne en externe communicatie.

Neem geen vertrouwelijke gegevens op in producten (rapportages, presentaties, etc.) die toegankelijk zijn voor niet-bevoegde personen.

Toelichting

Advies. Bespreek je rapportage of presentatie met je direct leidinggevende en vraag om akkoord (zie gouden regel 1).

Toestemming MT-lid voor presentatie. Voordat je een presentatie aan niet-bevoegde personen geeft (bijvoorbeeld buiten de Belastingdienst), dien je hiervoor toestemming van jouw afdelingshoofd in het MT te krijgen.

Delen van slides en rapportages. Het is niet toegestaan om slides na een presentatie of rapportages te delen met toehoorders of derden buiten de Belastingdienst. Bij het delen met personen buiten de Belastingdienst is niet duidelijk wat er met de presentatie gebeurt en is het niet mogelijk om toelichting te geven. Er kunnen altijd uitzonderingen worden gemaakt, bijvoorbeeld voor kennisdeling met buitenlandse Belastingdiensten. Voor uitzonderingen is toestemming nodig van jouw afdelingshoofd in het MT. Het is wel toegestaan om presentaties en rapportages binnen de Belastingdienst te delen. Bij het delen van een presentatie moet een disclaimer wordt toegevoegd, waarin staat dat een presentatie niet op zichzelf staat en dat een mondelinge toelichting van de betrokkenen essentieel is om een goed begrip te krijgen van de inhoud.

Alternatieve gegevens. Als het handig is om persoons- en bedrijfsgegevens weer te geven in een rapportage, presentatie of ander product, dan moet dit geanonimiseerd of gemaskeerd zijn. Bijvoorbeeld:

A.B. Persoon Straatweg 123 9999ZZ Dorpstad

Openbare informatie. Alle openbare informatie (bijvoorbeeld informatie die op de website van de Tweede Kamer te vinden is) mag gedeeld worden buiten de Belastingdienst.

Werking signaalmodellen. In een rapportage, presentatie of ander product mag de generieke werking van een signaalmodel worden beschreven, maar niet de specifieke werking van signaalmodellen die in ontwikkeling of in productie zijn.

Praktijkvoorbeelden

- In een presentatie voor een groep studenten mogen geen persoonsgegevens uit bronsystemen worden getoond. Deze informatie moet worden gemaskeerd door een zwarte balk of kruisjes of er moet fictieve data worden getoond.
- Een gebruikershandleiding voor DM/DI die breed wordt verspreid mogen geen fiscale gegevens zijn opgenomen die herleidbaar zijn naar een persoon of bedrijf.
- Voor de uitleg van de werking van een risicomodel mag geen bestaand model met voorspellende attributen worden getoond. In dat geval is het beter om een fictief voorbeeld te geven. Bijvoorbeeld: om schooluitval te voorspellen worden 100 attributen over kinderen, ouders en scholen verzameld en geanalyseerd. Uit de modelscore blijkt dat vooral de grootte van de school, het opleidingsniveau van de ouders en het aantal leerlingen in de klas goede voorspellers zijn voor uitval.

- Ga er bij een presentatie buiten de Belastingdienst vanuit dat er iemand als een journalist in de zaal zit. Bedenk dan welke gegevens zij wel en niet mogen zien of horen.

Gouden regel 5: Doelbinding.

Gebruik alleen gegevens die geoorloofd zijn voor de uitvoering van je werk.

Toelichting

Vaststellen doelbinding. Hanteer de beslisboom voor Green Lane toetsen, WMK-toetsen en PIA's om doelbinding te kunnen vaststellen (zie ook T-23 in het QA framework). Gebruik voor een project of product alleen gegevens die zijn verzameld met een verenigbaar doel als waar je deze gegevens voor wil gebruiken.

Ongeoorloofde gegevens. Het gebruik van bijzondere persoonsgegevens zoals (afgeleide) gegevens over iemands ras, nationaliteit of etnische afkomst, politieke overtuiging, godsdienst of levensbeschouwelijke overtuigingen, lidmaatschap van een vakbond, genetische of gezondheidsstatus, of seksuele gerichtheid is in principe niet toegestaan, tenzij dit expliciet wordt goedgekeurd in een PIA (privacy impact assessment).

Correlatie. In signaalmodellen is het mogelijk dat een bepaalde variabele in zichzelf wel geoorloofd is, maar sterk correleert met een ongeoorloofde variabele. Daardoor kan het zijn dat een signaalmodel altijd een specifieke doelgroep aanwijst. Dit soort zaken wordt gecontroleerd in een PIA (privacy impact assessment).

Praktijkvoorbeelden

- Vraag je af of zorgtoeslag en aftrekposten (indirect) iets zeggen over iemands gezondheidstoestand. Mag je deze dan nog gebruiken in analyses? Zorgtoeslag mag, want de hoogte van de toeslag zegt iets over de hoogte van het loon en niet over de gezondheid zelf. Aftrekposten is afhankelijk van het doel van de analyse, dus dit wordt beoordeeld in de PIA.
- Je mag de datakwaliteit van FLG niet valideren met gegevens uit UWV Polis omdat die gegevens voor een ander doel geleverd worden. Om dezelfde reden mag je SAP-gegevens niet gebruiken om data uit BvR te valideren.

Gouden regel 6: Dataminimalisatie.

Gebruik niet meer gegevens dan die noodzakelijk zijn voor de uitvoering van je werk.

Toelichting

Doelbeschrijving. Zorg voor een heldere doelbeschrijving van je project of analyse. Hieruit moet volgen welke gegevens minimaal noodzakelijk zijn voor het bereiken van dit doel. Hou er rekening mee dat je bij faseovergangen of na eenmalige analyses via een QC-proces (Quality Control) verantwoording moet afleggen over de manier waarop je dataminimalisatie hebt toegepast.

Advies. Blijf voortdurend in discussie over deze regel met je opdrachtgever, je collega's, je direct leidinggevende en de DPO.

Noodzakelijke gegevens. Selecteer alleen relevante variabelen en records bij de uitvoering van analyses. Minimaliseer dus zowel in de lengte als in de breedte.

Noodzaak per fase. In verschillende fases van een analyse of project kunnen verschillende gegevens noodzakelijk zijn. In de verkenning of labfase kan het nodig zijn om veel gegevens te gebruiken omdat nog onduidelijk is welke gegevens relevant zijn. Om dit te faciliteren is ook de aparte LAB-omgeving op SAS Grid ingericht. Werk in elke fase van je analyse of project met de minimale hoeveelheid gegevens.

Driedagenchallenge. Een driedagenchallenge wordt gezien als een experiment in een labomgeving. Daarom geldt de richtlijn van dataminimalisatie in beperkte mate voor driedagen challenges. De driedagen challenges worden in apart datagebied uitgevoerd en na afloop wordt dit datagebied geschoond.

Peer review. Gebruik review van collega's om je eigen oordeel van 'noodzakelijk' telkens te valideren. Blijf ook je collega's bevragen of ze hebben nagedacht over dataminimalisatie. Valideer hierbij zowel de code als het resultaat van een analyse of product.

Testdata. Gebruik waar mogelijk specifieke testdata en geen productiedata om je producten te testen. Het onderzoeken en creëren van bruikbare testdata (bijvoorbeeld via pseudonimisering) is in gang gezet.

Praktijkvoorbeelden

- Als je de vraag krijgt om loongegevens van een bsn op te sturen, neem dan niet overige gegevens als naam of woonplaats mee in je query.
- Gebruik zoveel mogelijk *SELECT kolom1, kolom2 FROM X* in plaats van *SELECT * FROM X*.
- Als je analyse of product gegevens toont van een specifieke groep klanten, neem dan vanaf het begin alleen die groep klanten mee in je analyse.
- Tijdens de ontwikkeling van een risicomodel wordt een ABT (analytical base table) gebouwd met daarin duizenden variabelen die mogelijk voorspellend zijn. Het definitieve voorspelmodel blijkt uiteindelijk slechts enkele honderden van deze variabelen te gebruiken. Als dit model naar productie gaat, is het dus niet meer nodig om alle niet-voorspellende variabelen óók te draaien.
- Als je data vanaf het internet haalt, dan is het vaak niet mogelijk om direct alleen de noodzakelijke gegevens op te slaan. Zorg er dan voor dat dit is beschreven in de doelbeschrijving van je analyse en zorg dat je zo snel mogelijk de niet-noodzakelijke gegeven verwijdert van onze omgeving.

Gouden regel 7: Persoonsgegevens raadplegen.

Het raadplegen van persoonsgegevens mag enkel een zakelijk doel hebben binnen de context van je onderzoek. Je mag geen gegevens van jezelf of je persoonlijke omgeving raadplegen (bijv. partner, familie, collega, huisgenoot, buren, dienstverlener, etc.). Tenzij dit expliciet uit de opdracht blijkt, mag je niet gericht zoeken naar specifieke bedrijven of personen met een vooraanstaande functie (bijv. VIPs, dienstverleners, bestuurders van beursgenoteerde bedrijven, etc.).

Toelichting

Subsidiariteit. Vanuit o.a. het subsidiariteitsprincipe is het nagenoeg niet te beargumenteren dat je voor de uitvoering van je werk gegevens over jezelf, je partner, buren of collega moet raadplegen. Omdat je gegevens op kúnt zoeken, wil niet zeggen dat je gegevens op mág zoeken.

Deskundigen. Raadpleeg deskundigen over hoe business rules, modellen, datafundamenten of producten getest of gevalideerd kunnen worden en leg testgevallen vast.

Onverwachte confrontatie. Het kan voorkomen dat je onverhoopt geconfronteerd wordt met gegevens van bovenstaande natuurlijke en niet-natuurlijke personen. Meld dit direct bij je direct leidinggevende.

Inzagerecht. Het argument 'dat je inzagerecht hebt in je eigen gegevens' kun je niet inzetten om je persoonlijke gegevens op te zoeken. Hiervoor zijn reguliere, wettelijk geldende procedures en behoor je te handelen zoals elke andere burger.

Outliers. Je mag outliers of andere bijzondere gevallen uiteraard analyseren.

VIP's. Een VIP is in de context van de Belastingdienst een persoon die op de VIP-lijst voorkomt in verband met bijvoorbeeld het bekleden van bepaalde publieke functies of leden van het Koninklijke Huis. De gegevens van deze personen zijn alleen zichtbaar voor een zeer select en daartoe expliciet daartoe geautoriseerde groep Belastingdienstmedewerkers. De indicatie VIP ligt vast in BvR.

Praktijkvoorbeelden

- Je mag outliers nader analyseren: indien in je product bijvoorbeeld een gezin met 20 kinderen voorkomt en dit is gegeven de context onwaarschijnlijk, dan mag je dit nader onderzoeken.
- Je mag niet de WOZ-waarde van je eigen huis opzoeken omdat je die nodig hebt voor je aangifte inkomstenbelasting. Hiertoe dien je je gemeente of de WOZ-lijn te benaderen.
- Je mag geen gegevens raadplegen van schildersbedrijven om een offerte aan te vragen / te beoordelen.
- Je mag geen gegevens van jezelf, je gezin, je buren raadplegen om een business rule te valideren.
- Je mag niet je eigen risicoscore uit het IH-risicomodel inzien.
- Je mag geen gegevens van je collega's opzoeken in BvR, DACAS of welk ander systeem dan ook, zelfs niet met toestemming van die collega.
- Je mag geen personen raadplegen met een onwaarschijnlijk hoog inkomen met als doel om uit nieuwsgierigheid informatie over VIP's of andere bekende Nederlanders op te zoeken.

Gouden regel 8: Wachtwoorden.

Werk altijd met je eigen wachtwoord. Leen je wachtwoord(en) nooit uit en schrijf ze niet op. Neem geen wachtwoorden op in programmatuur.

Toelichting

Inloggen voor collega. Log niet voor een ander in op de analyseomgeving.

DWB delen. Laat collega's niet op jouw DWB werken en werk niet op de DWB van een collega.

Wachtwoord in code. Het is niet toegestaan om persoonlijke accounts (username – wachtwoord) in programmatuur op te nemen, ook al is het wachtwoord encrypted[1]. Gebruik als alternatief systeem- of functionele accounts om wachtwoorden op te nemen in programmatuur of om query's te schedulen.

Groepsaccount. Het is niet toegestaan om vertrouwelijke informatie beschikbaar te stellen en/of te raadplegen onder een groepsaccount[2]. Daarmee is namelijk niet te herleiden wie deze informatie kan raadplegen en/of heeft geraadpleegd.

Tip! Met de applicatie *Keepass* kun je je wachtwoorden eenvoudig beheren.

Praktijkvoorbeelden

- Het is niet toegestaan om aan een nieuwe medewerker je wachtwoord uit te lenen zodat hij/zij alvast aan het werk kan.

[1] Dit wordt nu nog toegepast (o.a. OB negatief): er wordt aan een oplossing gewerkt.
[2] Dit wordt nu nog toegepast (o.a. Inzicht): er wordt aan een oplossing gewerkt.

Gouden regel 9: Wees iBewust.

Houd er rekening mee dat er zowel op kantoor als daarbuiten onbevoegden kunnen meeluisteren en –kijken met je werkzaamheden.

Toelichting

Cursus iBewustzijn. Als het goed is, heb je de online cursus iBewustzijn gevolgd bij de Belastingdienst Academie. Zorg dat je je houdt aan de richtlijnen die daar worden voorgeschreven.

Vergrendel je schermen en systemen. Dit geldt voor je al je devices (DWB, tablet en smartphone) en op alle locaties (op kantoor, in de trein, thuis, etc.).

Tip! Gebruik de combinatie Windows – L om onmiddellijk je DWB te vergrendelen.

Beveiligingskabel. Werk je op je DWB buiten een Belastingdienstlocatie, zorg dan dat je DWB via een beveiligingskabel aan je bureau of een ander vast punt is bevestigd. Een uitzondering geldt voor je eigen huis: daar is een beveiligingskabel niet verplicht. Bewaar je DWB daar wel uit het zicht als je hem niet gebruikt.

Meekijken. Je bent zelf verantwoordelijk voor de gegevens op je scherm. Zorg dat er geen onbevoegden op je scherm kunnen meekijken. Dit geldt voor zowel voor openbare plekken, thuis, als ook op kantoor.

Hardop spreken. Bespreek in een openbare ruimte geen vertrouwelijke informatie. Daarmee voorkom je dat onbevoegden toegang krijgen tot deze informatie.

Clean desk policy. Clean desk policy houdt in dat er geen informatie in onbevoegde handen kan komen (geen documenten laten liggen, vergrendel je schermen, etc.). Het uitgangspunt van clean desk is dat een werkplek (bureau) aan het eind van een werkdag of als je werkplek tijdelijk verlaat leeg en netjes wordt achtergelaten.

Whiteboard. Laat het whiteboard na een meeting schoon achter.

Papier. Je bent zelf verantwoordelijk voor je hardcopy's. Zorg dat hand-outs, geprint materiaal en je aantekeningen(boekje) niet in handen komen van onbevoegden.

Praktijkvoorbeelden

- Indien je met meerdere collega's een casus bespreekt achter je scherm sluit dan de applicaties waar persoonsgegevens inzichtelijk zijn indien deze niet relevant zijn voor het werk.
- Als je in de trein met collega's over werk praat, noem of toon dan geen vertrouwelijke gegevens, omdat onbevoegden kunnen meeluisteren of meekijken.
- Berg je notitieboekjes op in je kluis als je in de pauze naar buiten gaat.

Gouden regel 10: Denk mee.

Ben actief en kritisch bezig met de gouden regels en spreek collega's aan als ze ervan afwijken.

Toelichting

Discussieer mee. Als je vindt dat de gouden regels kunnen worden verbeterd (bijvoorbeeld als ze je belemmeren in je dagelijkse werk, als ze onduidelijk zijn of als er onderwerpen ontbreken), laat dit dan weten op het discussieforum over gouden regels.

Spreek collega's aan. Als je merkt dat collega's binnen DF&A zich niet aan de gouden regels houden, spreek ze hier dan op aan.

Blijf op de hoogte van wijzigingen. Wijzigingen in gouden regels worden altijd gecommuniceerd via e-mail en in weekstarts. In teamoverleggen staan de gouden regels ook periodiek op de agenda. Zorg dat je altijd op de hoogte bent van de meest recente gouden regels.